(51) International Patent Classification[7]: **H04L 9/00**

(21) International Application Number: PCT/US03/03993

(22) International Filing Date: 10 February 2003 (10.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/074,583 12 February 2002 (12.02.2002) US

(71) Applicant: **GOLDMAN, SACHS & CO.** [US/US]; One New York Plaza, New York, NY 10004 (US).

(72) Inventor: **YOUNG, Carl**; 85 Broad Street, NY 10004 (US).

(74) Agent: **KINCART, Joseph, P.**; Clifford Chance US LLP, 200 Park Avenue, New York, NY 10166 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: AUTOMATED SECURITY MANAGEMENT
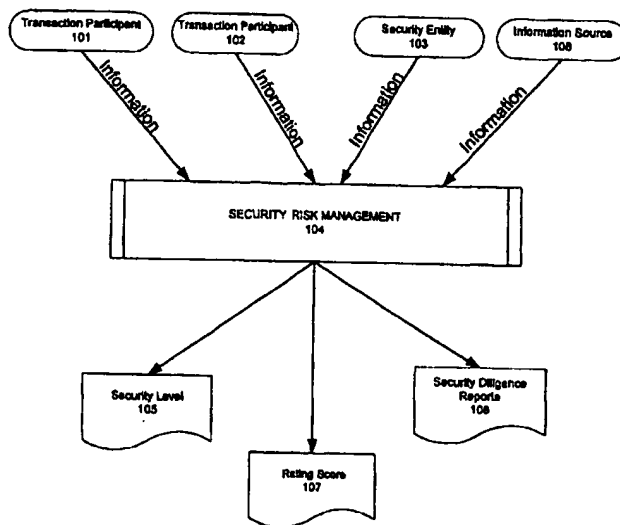
(57) **Abstract:** A computerized method and system for managing security risk, where risk associated with a breach of security is analyzed and quantified according to weighted risk variables. The analysis is accomplished by a computerized security risk management system (104) that receives information relating to physical, informational(108), communication and surveillance risk, and structures the information such that it can be related to risk variables and a security risk level can be calculated according to a relevance of associated risk variables. The security risk level(105) can be indicative of a likelihood that a breach of security may occur relating to a particular transaction (101) or facility. Similarly, a security confidence level can be indicative of how secure a particular facility or practice is and a security maintenance level can be indicative of a level of security (105) that should be maintained in relation to an analyzed subject.

they are aware of effective security measures, there can be uncertainty surrounding when it becomes appropriate to implement such security measures.

Effectively determining appropriate security actions can be complicated. Risk variables, such as a geographic location and a type of computer network may seem
5   completely unrelated to a layman business manager. However, a security expert may be concerned about a certain type of computer network, such as a wireless network, in an urban setting comprising multiple tenants and high pedestrian traffic. In the urban setting, the network may be more susceptible to violation, such as by a neighboring tenant, a pedestrian, or even a party in a neighboring building. Similarly, risk associated with a wireless network
10 may be almost non-existent in a suburban office park setting occupied by a homogeneous tenant. Relationships between individual risk variables can require sophistication and know how far beyond the scope of an average business manager.

In addition, it would be helpful to be able quantify what measures are taken or to reassure a potential business partner with an upfront commitment to a level of security that
15 will be applied to a business situation.

SUMMARY

Accordingly, the present invention provides a method and system for facilitating the management of security risk by identifying risk parameters that may seem unrelated, but have the potential to add to the overall level of risk. More specifically, the present invention
20 provides for a method and system to analyze and quantify a security risk and indicate appropriate actions to address the risk. An automated security risk management (SRM) system receives information which is utilized to quantify criteria relating to physical informational, communication and surveillance risk. A security risk level is calculated using the structured information such that it is indicative of the magnitude of the consequences
25 should a breach of security occur related to an event.

The present invention includes a computer-implemented method for managing risk related to a security risk event. Information relating to a security risk event is received by a computerized system which can structure the information received according to risk variables. The computerized system can also calculate a security level using the structured
30 information and a set of relationships established between the risk variables.

2

The security level can include an indication of an amount of risk that a breach of security may occur relating to the security risk event, a security confidence level indicative of how secure a particular facility can be made relative to a particular security risk event, a security confidence level indicative of how secure a particular practice can be made relative

5   to a particular security risk event or a security maintenance level indicative of a level of security that should be maintained in relation to an analyzed security risk event.

A suggested security measure can also be generated according to the security level and structured information. The suggested security measure can include, for example, physical protection of media containing information relating to the transaction, physical

10 protection of a facility or building associated with the security risk, or notifying an authority regarding potential breach of security.

The suggested security measure and the security level calculated can be stored and utilized for reporting.

In another aspect of the invention, branding can be associated with the suggested

15 security measure according to the set of relationships between the risk variables. Similarly, a level of analysis utilized in the calculation of the security level can be rated according to a classification.

The calculation can include a level of weighting associated with a category of risk variables, aggregating multiple weightings of risk variables, a relationship algorithm that

20 determines which variables effect other variables or a relationship algorithm setting forth how data included in a first variable can effect a weighting for a second variable. The security level can also be recalculated responsive to new information received or responsive to a progression of a chronology of events.

In another aspect, a computer system for providing security risk management can

25 include a computer server that is accessible with a network access device via a communications network and executable software stored on the server and executable on demand via the network access device. The software is operative with the server to receive information relating to security risk management criteria and calculate a security risk level.

Other embodiments can include a computer executable program code residing on a

30 computer-readable medium or a computer data signal embodied in a digital data stream.

Various features and embodiments are further described in the following figures, drawings and claims.

DESCRIPTION OF THE DRAWINGS

5   Fig. 1 illustrates a block diagram which can embody the present invention.

Fig. 2 illustrates a network on computer systems that can embody a security risk management system.

Fig. 3 illustrates a flow of exemplary steps that can be executed in practicing security risk management.

10   Fig. 4 illustrates an exemplary graphical user interface that can be utilized with the present invention.

DETAILED DESCRIPTION

15

The present invention includes a computerized method and system for managing security risk, including risk related to physical, informational, communication and surveillance. Risk associated with a breach of security is analyzed and quantified according to weighted risk variables. The analysis is accomplished by a computerized security risk

20   management (SRM) system 104 which receives information relating to physical and surveillance risk and structures the information such that it can be related to risk variables and a security risk level can be calculated according to a relevance of associated risk variables. The security risk level can be indicative of the amount of risk that a breach of security may occur relating to a particular event or facility. Similarly, a security confidence

25   level can be indicative of how secure a particular facility or practice can be made relative to a particular security risk event and a security maintenance level can be indicative of a level of security that should be maintained in relation to an analyzed security risk event or other risk subject.

Referring now to Fig. 1, a block diagram of one embodiment of automated security

30   risk management is illustrated. According to the present invention, a security risk level, a security confidence level, a security maintenance level, or other security related level

(Security Level) is calculated by a SRM system 104. One or more transaction participants 101-102, security entity 103, information source 108 or other entity, input information relating to an event, facility or other subject for which a Security Level 105 is to be determined. The SRM system 104 receives the information and structures it according to security risk variables. Programmable logic is utilized to analyze the structured information according to defined relationships between the variables.

For the purposes of this application, an event can include any quantifiable phenomenon from a single transaction, such as a transfer of currency, to an entire process, such as a merger of two corporate entities. A security risk variable can include any datum wherein a change in the value of the datum can cause a change in an amount of risk.

For example, information can be entered prior to a party commencing some action or as an action progresses and causes a change in one or more conditions or variables. In one embodiment, the information can be entered in response to questions or prompts such as into a form on a graphical user interface (GUI). In another embodiment, information can be entered in free text, or scanned from documents. Once entered, the information can be parsed and analyzed with software programs, such as artificial intelligence programs in order for the information to be automatically associated with defined variables. In the event that received information is not associated with a question or prompt and also cannot be automatically associated with any defined variables, the information can be flagged and forwarded to an operator or security personnel. The security personnel can then make a manual association with a defined variable, or create a new variable and also define relationships of the new variable with other known variables.

Other relationships between variables can be predefined and programmed into executable software code. The predefined relationships can be the result of historical effects one set of datum can have upon another. In addition relationships can be formulated according to a conclusion drawn from an expert in an appropriate field of endeavor. In one embodiment, branding can take place such that a set of relationships between variables can be referred to by name. A reputation associated with a particular name can be utilized to add credibility to an analysis of a set of data, including a security level calculated and a suggested security measure generated.

For example, if XYZ Security Company has an excellent reputation based upon many years of service in the security industry, the XYZ Security Company may certify an analysis

program that makes use of relationships between variables according to the expertise and experience of the XYZ Security Company or that a calculation is an XYZ calculation.

In another example, an analysis program can be rated according to how extensive an analysis will be performed upon a set of data. In this embodiment, normal day to day operations may be subjected to a moderate amount of analysis and processing. However, a very important or suspect subject may be subjected to a more extensive analysis. If desired, different levels of analysis can classified according to rating, such as, for example, a Class A rating may involve a most extensive analysis of a set of variables whereas a Class B rating correlate to a more moderate analysis and a Class C rating may correlate with a cursory analysis. If desired, an industry standard referring to risk classes can be established.

A Security Level 105 can be calculated as a result of the analysis of the variables. For example, a numerical value or other scaled weighting can be associated with particular information associated with a variable, wherein the scaled weighting is representative of risk associated with information being associated with that variable. In addition the scaled weighting can be adjusted higher or lower, or otherwise re-weighted, depending upon information received that relates to another risk variable if the risk variables can have an effect upon each other. In this manner complex associations and can be developed between variables, and algorithms can be developed that reflect those associations.

For example, it may be determined that an urban location poses minimal risk, therefore this information is correlates with a low scaled weighting, or even a negative scaled weighting. However, if other information related to physical access control indicates that there are some weak aspects of physical access control, the risk associated with the weak physical access may be further increased by the urban location. The scaled weighting for the weak access control may be increased, as well as the scaled weighting for the urban location. Similarly, a use of a wireless local area network (LAN) may carry a sustainable risk level and therefore be assigned a moderate scaled weighting. However if the wireless LAN is located in a shared facility with concealed areas that could surreptitiously house equipment capable of accessing the wireless LAN, the risk associated with the wireless LAN may be increased accordingly and a scaled weighting associated with the risk would also be increased.

If desired, an additional level of weighting can be assigned to a category of variables. For example, one category of variables may include background or situational information

6

and another electronic communications. A particular situation or transaction may place a much higher emphasis on security risk associated with the electronic communications variables. Therefore a category for the electronic communications variables would be assigned a higher rating. In one embodiment, logic embodied in computer code can

5   dynamically adjust both category and scaled variable weightings responsive to information received.

All weightings can also be aggregated into a subject rating score 107 that is indicative of a Security Level 104 associated with a scored subject, such as an event. For example, a single value can represent a security risk level associated with a particular transaction, or a

10   value may represent a security confidence level associated with a particular facility or corporate entity.

Relationship algorithms can include logic to determine which variables will effect other variables as well as how data entered for one variable will effect a weighting and value for another variable, such as whether data for one variable will increase risk or decrease risk

15   associated with another variable. A relationship algorithm can also include logic to determine the extent to which a value for one variable will effect risk when combined with a value for another variable.

In another aspect of the present invention, a transaction, or other subject, can be analyzed and a scored rating, or other Security Level 105 indicator, can be calculated that

20   indicates a level of security that should be maintained with an event. For example, information received by the SRM system 104 may indicate a high monetary value for a subject event. The subject event may also involve sensitive information that is subject to regulatory bodies, such as the Securities and Exchange Commission (SEC), for example, non-public material information relating to a corporate merger. Information can be received

25   into the SRM system 104 that describes the subject, the parties involved, effected entities, history of the effected entities, or any other pertinent data. The SRM system 104 can associate received information with risk variables and calculate a Security Level 105 that should be maintained with activity or information that relate to the subject event.

For example, if a merger or acquisition is going to take place that involves a Fortune

30   500 corporation, it may be very important to the participants that proprietary information relating to the acquisition be kept secret. The SRM system 104 can receive information

describing the acquisition situation and calculate a Security Level 105 that is indicative of minimum security requirements that need to be met until the occurrence of an intervening event, such as when the transaction is consummated, called off, made public, or other event.

A Security Level 105 for security maintenance can include guidelines for minimum
5   precautions that should be implemented, including security related to physical access to a facility, personnel involved, electronic communications, or any other security risk.

If desired, a Security Level 105 for a particular subject can be predetermined, such as by agreement of the participants. In this scenario, the SRM 104 can be utilized to process information relating to the subject and assure that the predetermined security level is being
10 adhered to. For example, a particular transaction may require a Security Level of 495 on a scale of 1 to 700, security measures that can support Security Level 495 or higher Security Level is then required. In the event that actual practices fail to sustain a predetermined level, the SRM 104 can suggest, and in some cases execute, an action commensurate with the failure.

15 It may also be appropriate for a Security Level 105 to change in response to new data received or as a chronology of events proceeds. For example, during the preliminary stages of merger negotiations, it may be extremely important to maintain a high level of security. However, a public announcement regarding the merger talks may put most of the material information into the public domain and therefore greatly reduce the need to maintain
20 stringent security measures.

In another aspect of the present invention, a rating can be utilized to indicate a level of security supported by a physical location, such as a building, a conference room, or other facility. This may include any variables that effect security of a facility, including physical access variables, perimeter security, internal security, electronic communication security, or
25 any other variables related to a physical location. In order to facilitate a choice of location for a subject transaction, a facility can be pre-qualified to support a level of security. In this manner, an appropriate facility in which work is to be hosted can be selected according to the maximum level of security the facility can support as well as the level of security required by the transaction.

30 The SRM 104 can also generate a suggested action that is responsive to a Security Level 104 or subject rating score 107. For example, in response to a high subject rating

8

score 107, a suggested action may suggest implementation of additional security measures at a particular facility, or even recommend a change in facility. In response to a low risk score, the SRM system 104 may respond by approving a current situation. Intermediate scores may respond by suggesting that additional information be gathered, or that minor changes be

5   made.

The SRM system 104 can also store, or otherwise archive SRM data, suggested actions and steps taken. This information can be useful to quantify corporate governance and diligent efforts to address high risk situations. For example the SRM system 104 can store information received, a Security Level 105, a rating score 107, and suggested actions to

10   be taken. Security diligence reports 106 quantifying risk management procedures, executed due diligence, corporate governance or other matters can be also be generated according to the stored data.

In another aspect of the present invention, automated actions can be executed by the SRM 104 in response to a security level for a subject that exceeds a predetermined

15   threshold, or if an actual breach of security is detected. Actions can include, for example, blocking access to documents or data relating to the transaction, encrypting electronic communications, generating an alert, notifying security personnel, or other appropriate response. In addition, the system can create a structured history relating to a particular transaction that can demonstrate due diligence and proper corporate governance. Reporting

20   can be generated from the structured history.

Referring now to Fig. 2, a network diagram illustrating one embodiment of the present invention is shown. An automated SRM system 104 can include a SRM Host 210 accessible via a distributed network 201 such as the Internet, or a private network. The SRM Host 210 can include a computerized server or other automated information sharing device.

25   A participant 101-102, security entity 103, or other party interested in security risk management can use a computerized system or network access device 204-208 to receive, input, transmit or view information processed in the SRM Host 210. A protocol, such as the transmission control protocol internet protocol TCP/IP can be utilized to provide consistency and reliability.

30   Each of the network access devices can include a processor, memory and a user input device, such as a keyboard and/or mouse, and a user output device, such as a display screen

and/or printer. The network access devices 204-208 can communicate with the SRM Host 210 to access data stored in databases 202 at the SRM Host 210. The network access device 204-208 may interact with the SRM Host 210 as if the host was a single entity in the network 201. However, the SRM Host 210 may include multiple processing and database sub-
5   systems, such as cooperative or redundant processing and/or database servers, which can be geographically dispersed throughout the network 201. In some implementations, groups of network access devices 204-208 may communicate with SRM Host 210 through a local area network.

The SRM Host 210 includes one or more databases 202 storing data relating to
10   restricted securities processing. The SRM Host 210 may interact with and/or gather data from a participant 101-102, security entity 103, other party interested in security risk management or any other person who is operating a network access device 204-208. Gathered data may be structured according to risk variables and utilized to calculate a Security Level 105.

15   An information provider server 211 can also be a source of information to a SRM Host 210. An information provider server 211 can include, for example, a news wire, quote system, commercial feed or source of information available electronically.

Typically a user will access the SRM Host 210 using client software executed at a network access device 204-208. The client software may include a generic hypertext markup
20   language (HTML) browser, such as Netscape Navigator or Microsoft Internet Explorer, (a "WEB browser"). The client software may also be a proprietary browser, and/or other host access software. In some cases, an executable program, such as a Java™ program, may be downloaded from the SRM Host 210 to the client computer and executed at the client computer as part of the SRM system software. Other implementations include proprietary
25   software installed from a computer readable medium, such as a CD ROM. The invention may therefore be implemented in digital electronic circuitry, computer hardware, firmware, software, or in combinations of the above. Apparatus of the invention may be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention may be
30   performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output.

Referring now to Fig. 3, managing security risk associated with a risk event can begin with opening a dialogue 310 between a SRM host 210 and a network access device 204-208. Typically, the dialogue would be opened by presenting a GUI to a network access device accessible by person who will enter information relating to the risk event. The GUI will be
5   capable of accepting data input via the network access device. An example of a GUI would include a series of questions relating to various aspects of security. If desired, the questions can be presented and answered via an online form.

Questions can relate to any aspect of security that might relate to the risk event, such as, for example: background and situational information, personnel security, physical access
10   and control, perimeter and internal security and electronic communications.

Alternatively, a dialogue can also be opened with a source of electronic data such as an external database or messaging system. For example, a news feed may include information relating to a change in management at a corporation, or a change in senior management. Other pertinent news items can include information relating to a government
15   list, a threat of violence, or information relating to state of the art security measures or equipment. In any case, the dialogue will facilitate the SRM system 104 receiving data relating to the risk event 311.

Security Risk variables associated with the risk event can be defined as well as relationships between various variables 312. Typically risk variables will be predefined by a
20   security expert or other knowledgeable person. Information that is received may relate to more than one variable and may be entered into more than one data field or have relational links to more than one data field. For example, a response to a question on how a company makes use of a private investigative firm may also relate to a data field pertaining to verification of statements on an employment application. Relationships between variables
25   can also be defined by the expert. Relationships can be multi-faceted and depend upon a value entered into a data field. For example, information received indicating that a company produces products with potentially adverse political implications may also relate to adequate physical security at a company facility.

Received information can be automatically associated with and structured to an
30   appropriate risk variable or multiple risk variables according to defined relationships 313.

Typically the relationships will be defined by the security expert. Association of received information to a risk variable can be accomplished via many well known methods of data field input including, for example: inputting a response to a question into one or more associated fields, key word association of received information with an appropriate field,

5   association of quantitative data according to threshold values, formatting data with a mask or any other means of associating received data with a pertinent data field.

In the event that information received is not readily associated with a pre-defined variable data field through an automatic process, a notification can be sent to a human operator to make an appropriate association. The human operator, such as a security expert,

10   can then define new variables and/or relationships as necessary 314. In this manner all of the data received as information can be associated with a risk variable and the risk variables can properly relate with one another.

The SRM system 104 can perform analysis on the risk variables 315 by processing relationships that have been defined in software logic code. As a result of the analysis 315, a

15   weighted value can be applied to the risk variables 316 such that a Security Level 105 can be calculated 317.

A suggested action that is responsive to the Security Level 105 and risk variables can also be generated 318. For example, if a security risk level is high due to weakness in physical access control, the SRM System can flag this weakness and also suggest how to

20   improve the control over physical access. In another example, if a risk event includes a pending financial transaction, such as a corporate merger, and there is a substantial profit or regulatory risk if details are disclosed, a relatively high security maintenance level may be calculated. This security maintenance level can be associated with a predefined operating standard 319. The operating standard can dictate guidelines relating to as many aspects of

25   security as are appropriate. For example, only encrypted electronic communications may be acceptable for any communications relating to the subject. In addition, a facility that includes secured physical access, hardwired local area networks and interior meeting space may also be required in order to comply with the predefined operating standard.

A security risk diligence report can be generated 320 wherein the report can capture

30   the risk event, variable analysis, Security Level 104 and suggested actions and other pertinent

data. A diligence report can be useful to demonstrate good corporate governance and proper handling of security risk. The diligence report can also serve as an archival system in order to memorialize security measures taken.

Referring now to Fig. 4, an exemplary GUI for receiving security risk related

5   information is illustrated 400. The GUI can include areas prompting for information, such as in the form of a question 401 and appropriate responses 402. A programmable user interactive device 403-405, such as a checkbox, X field, yes/no filed or other device can be utilized to indicate an answer, or otherwise input information. A category weighting 407 can also be indicated on the GUI. Typically the weighting will be predetermined. However,

10   if desired the weighting can be modified by a user.

A GUI 400 can also include areas for displaying a Security Level 406 and an area for displaying a suggested action 408. Other features that can be presented in a GUI include a report, a summary of activity, an operating standard or other related subject matter.

A number of embodiments of the present invention have been described.

15   Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. For example, a network access device 204-208 can comprise a personal computer executing an operating system such as Microsoft Windows™, Unix™, or Apple MacOS™, as well as software applications, such as a web browser. A network access device 204-208 can also be a terminal device, a palm-type

20   computer WEB access device that adheres to a point-to-point or network communication protocol such as the Internet protocol. Other examples can include TV WEB browsers, terminals, and wireless access devices (such as a 3-Com Palm VII organizer). Accordingly, other embodiments are within the scope of the following claims.

CLAIMS

What is claimed is:

1.   A computer-implemented method for managing risk related to a security risk event, the method comprising:

5   receiving information relating to a security risk event;

structuring the information received according to risk variables; and

calculating a security level using the structured information and a set of relationships established between the risk variables.

10   2.   The method of claim 1 wherein the security level comprises an indication of an amount of risk that a breach of security may occur relating to the security risk event.

3.   The method of claim 1 wherein the security level comprises a security confidence level indicative of how secure a particular facility can be made relative to a particular security

15   risk event.

4.   The method of claim 1 wherein the security level comprises a security confidence level can be indicative of how secure a particular practice can be made relative to a particular security risk event.

20

5.   The method of claim 1 wherein the security level comprises a security maintenance level indicative of a level of security that should be maintained in relation to an analyzed security risk event.

25   6.   The method of claim 1 additionally comprising the step of:

generating a suggested security measure according to the security level and structured information.

7.   The method of claim 6 additionally comprising the step of:

30   storing the information received, the security level and the suggested security measure.

14

8.   The method of claim 6 additionally comprising the step of:

        receiving information relating to security measures executed; and

        generating a security diligence report.

9.   The method of claim 8 wherein the security diligence report comprises inquiries made relating to the security risk event and security measures executed responsive to the security level.

10.   The method of claim 6 wherein the suggested security measure comprises physical protection of media containing information relating to the transaction.

11.   The method of claim 1 wherein the suggested security measure comprises physical protection of a facility associated with the security risk.

12.   The method of claim 1 wherein the wherein the suggested security measure comprises physical protection of a building associated with a business transaction.

13.   The method of claim 1 wherein the suggested action comprises notifying an authority regarding potential breach of security.

14.   The method of claim 6 additionally comprising the step of:

        branding the suggested security measure according to the set of relationships between the risk variables.

15.   The method of claim 1 wherein level of analysis utilized in the calculation of the security level is rated according to a classification.

16.   The method of claim 1 wherein the calculation comprises a level of weighting associated with a category of risk variables.

17.   The method of claim 1 wherein the calculation comprises aggregating multiple weightings of risk variables.

18.   The method of claim 1 wherein the calculation comprises a relationship algorithm that
5   determines which variables effect other variables.

19.   The method of claim 1 wherein the calculation includes a relationship algorithm comprising how data comprising a first variable can effect a weighting for a second variable.

10   20.   The method of claim 1 additionally comprising the step of:
        recalculating the security level responsive to new information received.

21.   The method of claim 1 additionally comprising the step of:
        recalculating the security level responsive to progression of a chronology of events.
15

22.   A computerized system for managing risk related to a security risk event, the system comprising:
        a computer server accessible with a system access device via a communications network; and
20   executable software stored on the server and executable on demand, the software operative with the server to cause the system to:
        receive information relating to a security risk event;
        structure the information received according to risk variables; and
        calculate a security level using the structured information and a set of relationships
25   established between the risk variables.

23.   The computerized system of claim 22 wherein the data is gathered via an electronic feed.

24.   Computer executable program code residing on a computer-readable medium, the program code comprising instructions for causing the computer to:

receive information relating to a security risk event;

structure the information received according to risk variables; and

calculate a security level using the structured information and a set of relationships established between the risk variables.

25.   A computer data signal embodied in a digital data stream comprising data relating to risk management, wherein the computer data signal is generated by a method comprising the steps of:

receiving information relating to a security risk event;

structuring the information received according to risk variables; and

calculating a security level using the structured information and a set of relationships established between the risk variables.

26.   A method of interacting with a network access device so as to manage risk relating to a risk subject, the method comprising the steps of:

initiating interaction with a security risk management server via a communications network;

inputting information descriptive of a security risk event;

transmitting the information descriptive of security risk event to a security risk management server; and

receiving a security level calculated using the information descriptive of a security risk event and a set of relationships established between risk variables associated with the information descriptive of a security risk event.

27.   The method of claim 35 wherein the risk event is a financial transaction.

28.   The method of claim 26 additionally comprising the step of receiving a suggested security measure according to the security level and structured information.
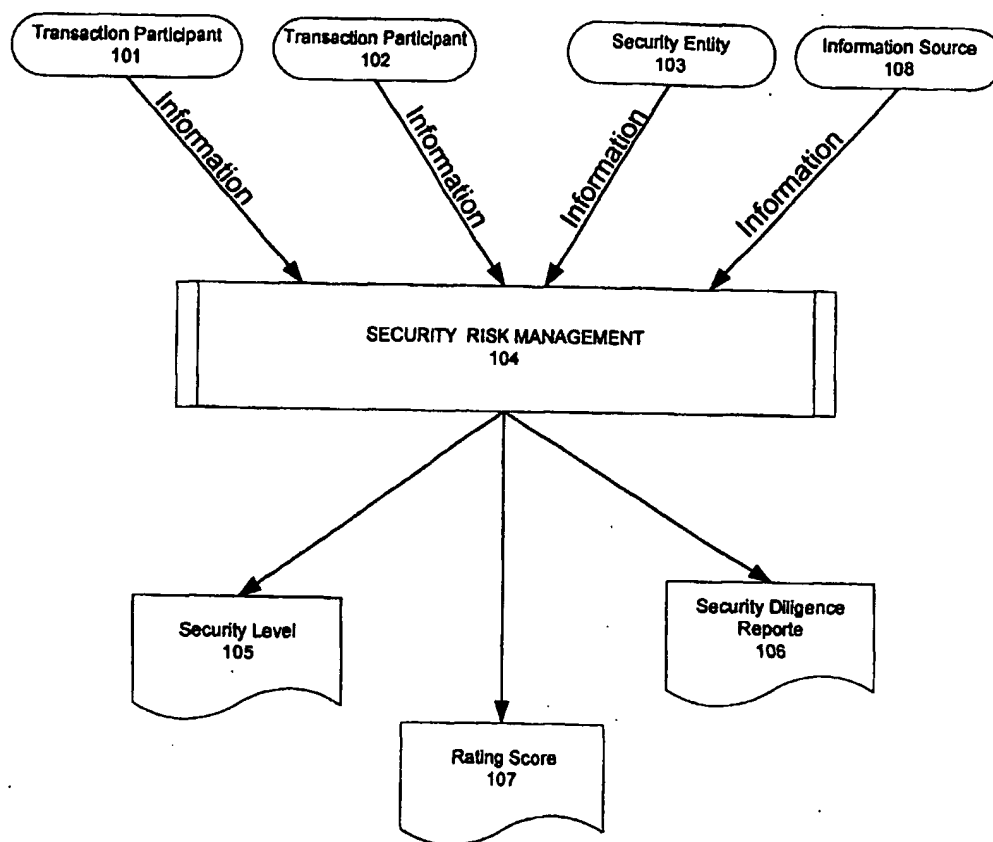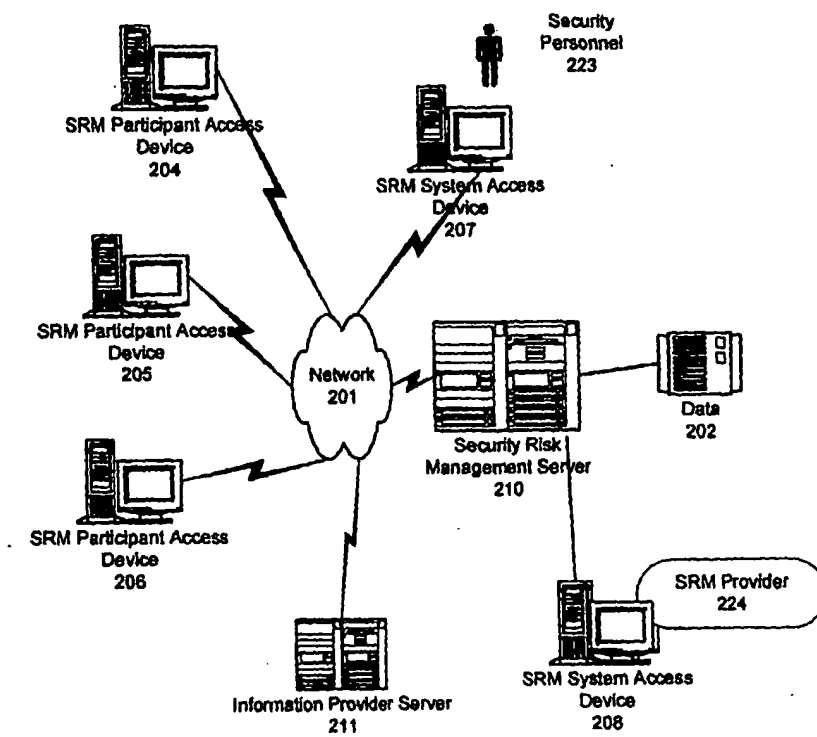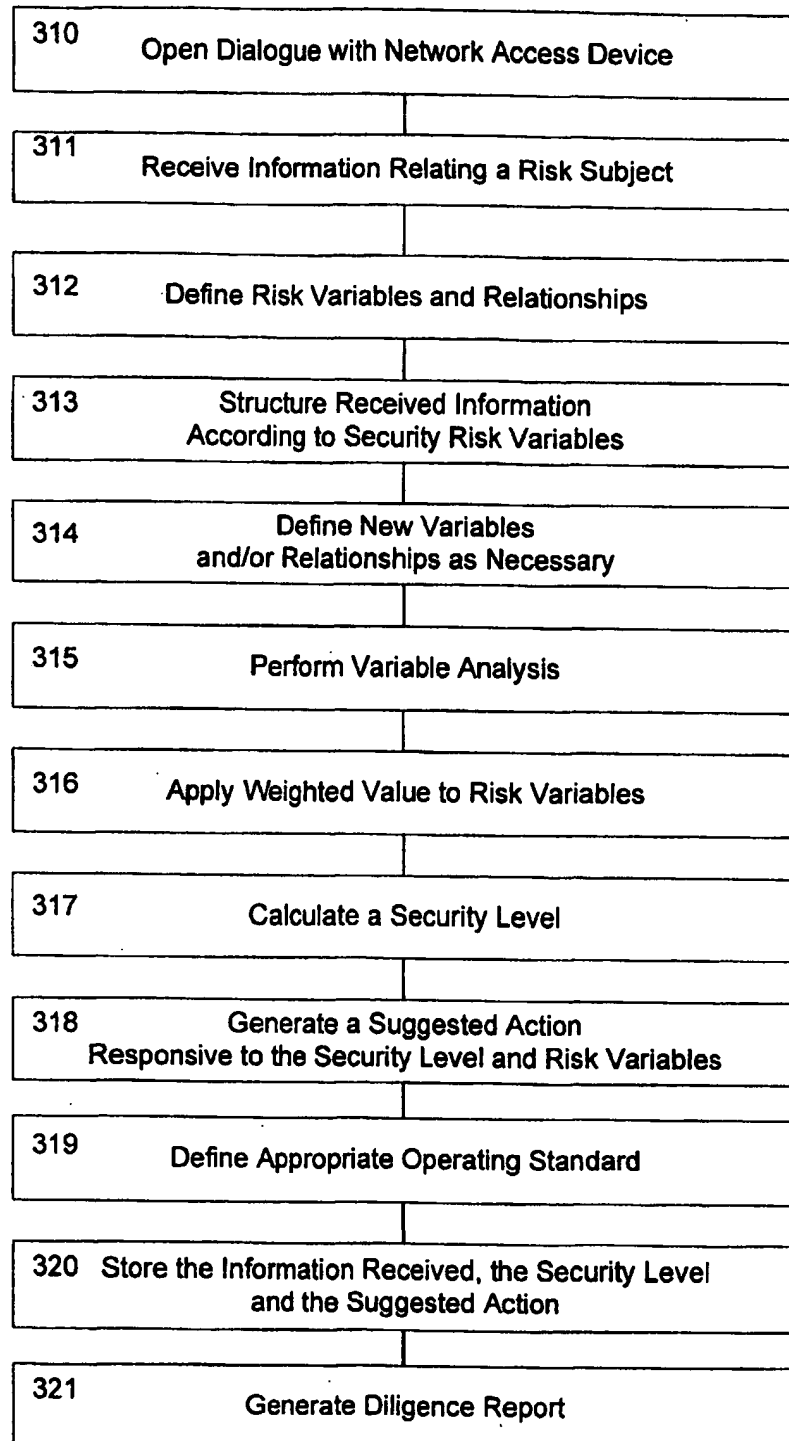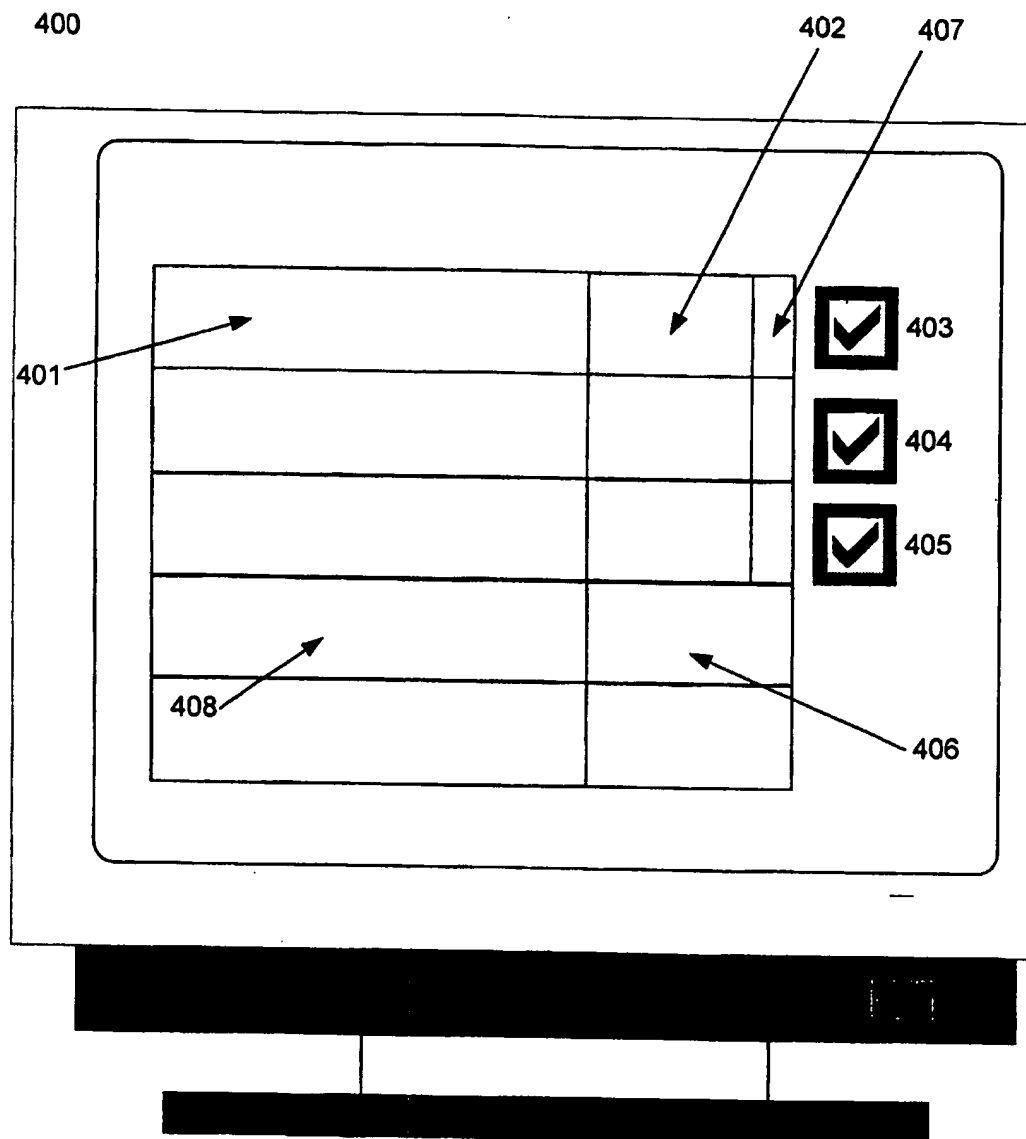
17

Fig. 1

Fig. 2

| 310 | Open Dialogue with Network Access Device |

| 311 | Receive Information Relating a Risk Subject |

| 312 | Define Risk Variables and Relationships |

| 313 | Structure Received Information According to Security Risk Variables |

| 314 | Define New Variables and/or Relationships as Necessary |

| 315 | Perform Variable Analysis |

| 316 | Apply Weighted Value to Risk Variables |

| 317 | Calculate a Security Level |

| 318 | Generate a Suggested Action Responsive to the Security Level and Risk Variables |

| 319 | Define Appropriate Operating Standard |

| 320 | Store the Information Received, the Security Level and the Suggested Action |

| 321 | Generate Diligence Report |

Fig. 3

Fig.4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/03993

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7)   :   H04L 9/00
US CL   :   713/201

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WEST, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,304,973 B1 (WILLIAMS) 16 October 2001 (16.10.2001), Abstract; fig.1, 2, 5 and 6; col.4, lines 24-67; col.5; col.6, lines 35-67; col.7-26.	1-28

☐ Further documents are listed in the continuation of Box C.   ☐ See patent family annex.

Date of the actual completion of the international search	Date of mailing of the international search report
20 May 2003 (20.05.2003)	0 2 JUN 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Gilberto Barron Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)